Transportation Security Administration

OFFICE OF INFORMATION TECHNOLOGY

TSA MANAGEMENT DIRECTIVE No. 1400.20
IT GOVERNANCE

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for the TSA Information Technology (IT) Governance framework.

2. **SCOPE:** This directive applies to all TSA employees and contractors.

3. **AUTHORITIES:**

   A. Clinger-Cohen Act of 1996, Public Law 104-106 (40 U.S.C. § 1401 et seq.)

   B. Cybersecurity Act of 2015, Sec. 225. Federal Cybersecurity Requirements

   C. *DHS Guide, EAB Governance Process Guide*

   D. *DHS MD 04000, Delegation for Information Technology*

   E. *DHS MD 102-01, Acquisition Management Directive*

   F. *DHS MD 102-01-103 Systems Engineering Life Cycle*

   G. *DHS MD 103-01, Enterprise Data Management Policy*

   H. *DHS MD 102-02, Capital Planning and Investment Control*

   I. *DHS MD 102-04 Portfolio Management*

   J. *DHS MD 142-02, Information Technology Integration and Management*

   K. *DHS 4300A, Sensitive Systems Handbook*

   L. Federal Information Technology Acquisition Reform Act, Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Public Law No. 113-291

   M. OMB Circular A-11, July 2016: Section 55 – Information Technology Investments

   N. OMB Circular A-130, Managing Federal Information as a Strategic Resources

   O. OMB Memorandum M-10-27, Information Technology Investment Baseline Management Policy

   P. OMB Memorandum M-15-11: Fiscal Year 2017 Budget Guidance

Q. OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology

R. OMB Memorandum M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops

S. OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government

T. OMB Memorandum M-16-12, Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing

U. OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response

V. OMB Memorandum M-16-20, Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services

W. *TSA MD 300.8, Acquisition Program Review and Reporting*

X. *TSA MD 300.12, Program Requirements Review and Approval*

Y. *TSA MD 300.15, Information Technology Acquisition Review*

Z. *TSA MD 1400.3, Information Technology Security*

AA. *TSA Information Assurance (IA) Handbook*

4. DEFINITIONS:

A. Acquisition Decision Authority (ADA): The individual, designated in accordance with criteria established by the DHS Chief Acquisition Officer, to approve entry of an acquisition program into next phase of the acquisition.

B. Acquisition Review Board (ARB): DHS or TSA executive board that reviews investments for proper management, oversight, accountability, and alignment to strategic functions of the Department.

C. Authority to Operate (ATO): The official management decision issued by a designated approval authority (DAA) to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

D. Authorizing Official (AO): Senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

E. Asset Management System: A property management application used to document, manage, and track the maintenance of assets currently owned by TSA.

F. Capital Planning and Investment Control (CPIC): An integrated process within an agency for planning, budgeting, procurement, and management of the agency's portfolio of capital assets to achieve agency strategic goals and objectives in support of agency missions and business needs with the lowest life-cycle costs and least risk.

G. Data Insertion (DI) Decision Request: A decision request for approval on the insertion of new data elements into the TSA and DHS Enterprise Architecture based on the content of the Data Reference Model (DRM).

H. Data Management (DM): The practice of putting into place policies, procedures and best practices that ensure data is understandable, trusted, visible, accessible, viable and interoperable. DM functions include processes and procedures that cover planning, modeling, security, information assurance, access control, and quality. Outcomes of DM include the improvement of data quality and assurance, enablement of information sharing, and the fostering of data reuse by minimizing data redundancy.

I. Data Management Plan (DMP): The DMP identifies the information needs, data requirements, data conversion, and data security strategies. The goals of data management include re-use of existing resources through the discovery of available data services and data repositories in order to provide timely, accurate information and supporting data protection.

Note**:** Project Staff need to know what data is available, the quality and how it's used, how to incorporate it into resource management decisions, and how it will be managed over time.

J. Decision Request (DR): A request for a decision related to a program, product or service approval.

K. Enterprise Architecture (EA): The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

(a) means – (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (b) includes – (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan (44 U.S.C. § 3601).

EA is the foundation for investment planning and decision-making. The architecture guides TSA's efforts in maximizing standardization and interoperability among information, business processes, and technology solutions. Additionally, the EA will be leveraged to enable the identification of redundant and inefficient systems and to ensure alignment and compliance with applicable laws, policies, and regulations to promote streamlined business operations.

L. Enterprise Architecture Framework (EAF): A structure for organizing information that defines the scope of the architecture (what will be documented) and how the areas of the architecture are related. (The OMB Common Approach to Federal Enterprise Architecture (CAFEA)). The EAF provides a common approach for the integration of strategic, business and technology management as part of organization design and performance improvement.

M. Enterprise Architecture Review Council (EARC): The EARC reviews all program requests and technical architecture changes and submits recommendation memorandums to the CIO at the TSA Information Technology Investment Review Board (ITIRB) for approval or rejection. Membership includes TSA OIT Division Directors, subject matter experts (as needed) in DM, EA, CPIC, Systems Engineering Lifecycle (SELC), and applicable Program or Project Managers. The EARC is chaired by the TSA Chief Architect.

N. Enterprise Risk Management: Is a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

O. Enterprise Risk Steering Committee (ERSC): Is responsible for establishes risk policies; identifying enterprise level risk to be placed on the enterprise risk register; approving mitigation strategies and controls for these risks; assigning a lead executive with responsibility for coordinating and reporting risks; reviewing the status and effect of approved mitigation strategies; approving and directing additional response actions when required; and integrating risk with TSA's strategy, budget planning, and resource-allocation decisions.

P. Federal Information Technology Acquisition Reform Act (FITARA): Outlines specific requirements related to: Chief Information Officer (CIO) authority enhancements; enhanced transparency and improved risk management in information technology investments; portfolio review; approval of contracts and agreements, expansion of training and use of information technology cadres; Federal Data Center Consolidation Initiative (FDCCI); maximizing the benefit of the Federal Strategic Sourcing Initiative (SSI); and the Government-wide software purchasing program.

Q. Future Year Homeland Security Program (FYHSP): Is a five-year resource plan that guides components on how to best achieve the agency's mission and goals outlined in the Strategic Plan within fiscal constraints.

R. Independent Government Cost Estimate (IGCE): The IGCE is the Government's estimate of the resources and projected cost of the resources a contractor will incur in the performance of a contract. These costs include direct costs such as labor, products, equipment, travel, and transportation; indirect costs such as labor overhead, material overhead, and general and administrative (G&A) expenses; and profit or fee (amount above costs incurred to remunerate the contractor for the risks involved in undertaking the contract).

S. Information Technology Architecture: The structure, processes, procedures, and design constraints in which TSA IT assets are produced in order to support the information requirements of the TSA enterprise that are aligned with the Enterprise Architecture.

T. Information Technology Governance: The management structure, responsibilities, and authorities of Heads of Departments and agencies and their CIOs to fulfill their

responsibilities in planning, acquiring, securing, operating, and managing all agencies IT resources.

U. Information Technology Investment: An investment, or portion of an investment, in a product or service that involves the development, maintenance, use of computer systems, software, and networks for the processing and distribution of data.

V. Information Technology Investment Review Board (ITIRB): A senior-level TSA agency-wide board of Assistant Administrators (AA), chaired by the TSA CIO. The ITIRB provides enterprise-wide, business-led support for business- and IT-related initiatives. The ITIRB ensures that all IT initiatives having cross-agency impacts affecting the IT infrastructure, common services and customer service programs are implemented to provide effective support for the TSA's business mission and operations. The ITIRB has primary responsibility for all stages of IT implementation, including: planning, prioritization, resource assignment, progress monitoring, evaluation, re-allocation, and termination of initiatives. It is also responsible for reviewing IT performance and evaluation criteria, measures and targets, adhering to Department acquisition and strategic sourcing policies, and to eliminate duplicative, enterprise-wide IT initiatives.

W. Internal Use Software (IUS): Software that is developed or purchased from commercial vendors or Government entities to (1) operate and support TSA's programs (e.g., project execution, financial, and administrative software, including that used for project management); (2) produce goods or to provide services; and (3) provide support to other Federal entities with or without reimbursement.

X. IT Source Selection Advisory Committee (SSAC): Provides Senior-level oversight throughout the Acquisition Life Cycle for technical review of every procurement, acquisition, or agreement that contains an IT element and recommends to the CIO for signature in accordance with the Federal Information Technology Acquisition Reform Act (FITARA)'s Common Baseline.

Y. Life-Cycle Cost Estimate (LCCE): The estimated cost of developing, producing, deploying, maintaining, operating and disposing of an authorized system over its entire lifespan. These costs include not only the direct costs of the initiative, but also include indirect costs that would be logically attributed to the initiative. In this way, all costs that are logically attributed to the initiative are included, regardless of funding source or management control. It is used to acquire funding for an authorized system throughout its lifespan.

Z. Planning, Programming, Budget and Execution (PPBE): DHS's cyclical, multi-year resource allocation process consisting of four phases: planning, programming, budgeting and execution. It is used to articulate goals and priorities, and develop and implement a program structure with phased financial resource and personnel requirements to accomplish goals and objectives.

AA. Portfolio Management: The management of broad investment categories linked by their relationship to the agency's mission to ensure effective performance, correspondence to the TSA and DHS EA, minimization of overlapping functions, and proper funding.

BB. Project Authorization Document (PAD): A request for OIT support on a project or initiative that requires OIT involvement. It provides high-level information about the initiative such as business requirements, estimated cost and a commitment of funds and resources.

CC. Program Alignment (PA) Decision Request: A decision request for approval on the alignment of program investments with the TSA and DHS EA and conformance with technology strategies and capabilities.

DD. Segment Architecture: Defines a simple roadmap for a core mission area, business service or enterprise service, aligning to the structure and artifacts of the enterprise architecture. A segment is a subset of the enterprise, either a core mission area, business service, or enterprise service, which brings an added level of detail to the EA for a portion of the enterprise.

EE. Service Insertion (SI) Decision Request: A decision request for approval on the insertion of new services into the TSA and DHS EA based on the content of the Service Reference Model (SRM).

FF. "Shadow IT" or "Hidden IT": Refers to spending on IT that is not fully transparent to the TSA CIO and/or IT resources included as a portion of a program that is not primarily of an "information technology" purpose but delivers IT capabilities or contains IT resources.

GG. Solution Architecture: Defines agency IT assets such as authorized applications, systems, networks, information, data, services, cloud, security or components used to automate and improve agency business functions, and describe system compatibility and the components, elements and core technologies required to deliver a solution.

HH. System Owner (SO): Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

II. Systems Engineering Lifecycle (SELC): A systems engineering framework for enabling efficient and effective delivery of capability to users, and is one of several key TSA and DHS processes for managing acquisitions of programs and their related projects. It serves as a structured approach to system development and refinement and is used from system inception to system disposal. The SELC defines the procedures, approvals, and artifacts required to incorporate authorized system modifications.

Note: In the context of information security requirements in acquisition, management, and disposition of IT products and services, TSA is required by FISMA to incorporate the requirements for information security into the SELC. Key Decision Point three (3) milestone in the SELC shall not be passed until the ATO for the information system is granted.

JJ. Technology Insertion (TI) Decision Request: A decision request for approval on the insertion of new or upgraded technologies into the TSA and DHS EA based on the content of the Technical Reference Model (TRM).

5. RESPONSIBILITIES:

A. The Component Acquisition Executive (CAE) is responsible for:

(1) Management and oversight of all TSA Acquisition functions;

(2) Establishing acquisition policy and processes within TSA;

(3) Serving as the Acquisition Decision Authority (ADA) for acquisitions managed at TSA;

(4) Serving as the TSA recommending official for DHS oversight acquisition programs;

(5) Serving as a member of ITIRB; and

(6) Coordinating with the CIO for review of all Acquisition Program contracts or agreements containing an IT element prior to award.

B. The Chief Information Officer (CIO) is responsible for:

(1) Serve as a member of governance boards that include IT resources (including "shadow IT" or "hidden IT"), including Investment Review Boards.

(2) Overseeing and ensuring proper execution of the IT Governance framework across TSA;

(3) Establishing the Component IT priorities, policies, processes, standards, guidelines, and procedures;

(4) Ensuring all TSA information systems undergo security assessment and authorization and obtain an Authorization to Operate (ATO) prior to operation and deployment. This includes all systems (including pilots) that connect to the TSA network or process TSA sensitive data;

(5) Ensuring that the Security Authorization Package and the Security Authorization Decision Letter (which contains the Authorization Decision, Decision Rationale, accepted Residual Risk level, and Terms and Conditions for Authorization) shall be routed from the system owner (SO) through the Security Control Assessor (SCA) to the Authorizing Official (AO) for ATO approval;

(6) Serving as the Chairperson for the ITIRB overseeing the management of the TSA's IT portfolios, and approving the allocation of IT resources to best achieve TSA strategic goals and objectives within budget limits;

(7) Collaborating with the CFO and the CAO in pre-budget submissions for programs that include IT and the overall portfolio throughout the planning, programming, and budgeting stages;

(8) Establishing and managing the IT Acquisition Review (ITAR) process to:

(i) review all acquisition requests and approve those that contain IT elements pre-solicitation;

(9) Review and approve all contracts and agreements with Information Technology by:

(i) ensuring IT representation on technical evaluation teams (TETs) for acquisitions containing IT elements; and

(ii) reviewing and approving all technical evaluation submissions and evaluation summaries developed by solicitation technical evaluation teams (TETs) before submission to the Source Selection Authority (SSA) for contracts and agreements containing IT elements. (actions coordinated with the Chief Acquisition Officer).

(10) Appointing, in consultation with the CAE, members of the IT Source Selection Advisory Committee (SSAC) to include at a minimum representation for Enterprise Architecture and Information Assurance;

(11) Leveraging Enterprise Architecture (along with Data Management) direction and portfolio analysis, to include Component/Program performance, to support leadership decisions;

(12) Providing primary input into the IT capital planning and investment control (CPIC) documents submitted with the agency budget;

(13) Approving the IT components of any plans through a process that balances IT investments with other uses of agency funding. This includes CIO involvement with planning for IT resources at all points in their lifecycle, including operations and disposition or migration;

(14) Reviewing, ensuring, and certifying that IT investments, and estimates for the IT related cost of all acquisitions plans and acquisition strategies, are using adequate incremental development principles;

(15) Reviewing, modifying, endorsing, or terminating, all acquisition strategies, acquisition plans or interagency agreements that include IT;

(16) Reviewing all cost estimates of IT related costs, both IGCEs and LCCEs, and ensuring all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles; and

(17) Establishing a Program Health Assessment process to periodically evaluate, including Program Manager engagement, the use of agency IT resources against applicable performance measurements, resulting in a decision to approve, continue, modify, pause, or terminate the resource expenditure.

C. The Chief Enterprise Architect (CEA) is responsible for:

(1) Ensuring alignment to TSA and DHS Enterprise Architecture under the direct authority of the TSA CIO;

(2) Chairing the TSA EARC and facilitating the Decision Request (DR) process;

(3) Chairing the IT Source Selection Advisory Committee (SSAC) meetings;

(4) Facilitating ITAR technical reviews and recommendations for all phases of Acquisition;

(5) Preparing recommendations to the TSA ITIRB for CIO certification;

(6) Ensuring the TSA ITIRB is briefed and kept informed on the issues and program reviews associated with the DHS EA Governance process;

(7) Creating and maintaining the TSA Enterprise Architecture (TSA EA) to include agency-wide sub-architecture domains (Strategic, Business Services, Data and Information, enabling applications, Host Infrastructure, and Security) core artifacts, and reference models in the FEA (e.g. BRM, SRM, DRM, TRM, and PRM) identified in OMB's "The Common Approach to Federal Enterprise Architecture (CAFEA)";

(8) Defining the TSA Segment Architecture for core mission areas, business services, or enterprise services; and

(9) Approving the TSA Information Technology Architecture, subordinate Solution Architectures, and ensuring alignment to the structure and artifacts of the agency's EA.

D. The Chief Financial Officer (CFO) is responsible for:

(1) Serving as a member of the TSA ITIRB;

(2) Ensuring resource alignment with TSA ITIRB and TSA ARB decisions;

(3) Coordinating with the mission area AAs to ensure the FYHSP reflects the current TSA acquisition program requirements;

(4) Accounting for IUS and to provide guidance for identifying, monitoring and accounting for capitalized IUS purchases at TSA, including software licenses that meet the capitalization criteria; and

(5) Coordinating with the CIO prior to reprogramming any funds associated with IT.

E. Assistant Administrators (AA) are responsible for:

(1) Serving as members of the TSA ITIRB;

(2) Serving as sponsors for requests that are generated from their specific organizational element;

(3) Ensuring each decision request reflects any impacts of program requirements in their specific mission area; and

(4) Ensuring that any required program designation decision is coordinated with the CIO and the CAE and will ensure compliance with the designation decision.

F. Program Offices, under the authority of the Program Manager (PM), are responsible for:

(1) Working with the CIO to define IT performance metrics and strategies to support fulfillment of agency strategic objectives as defined in TSA's strategic plan;

(2) Ensuring program alignment to the TSA EA;

(3) Ensuring compliance with the DM, EA, and SELC processes throughout each request's lifecycle and that all appropriate documentation has been completed;

(4) Documenting the Solution Architecture and developing investment solutions in adherence with the agency's EA and ITA;

(5) Ensuring investment and decision requests align with agency's mission and strategic plan while supporting its business needs, minimizing risks, and maximizing returns through the investments lifecycle;

(6) Ensuring there is adequate supporting information to account for IUS (including vendor and federal employee costs) and to document the key lifecycle phases for capitalized IUS purchases at TSA;

(7) Ensuring data calls for existing or potential IUS applications are reported to the Office of the Chief Information Officer to be included in the quarterly CIO Completeness Report;

(8) Ensuring impaired or decommissioned IUS assets are reported to the Office of Finance and Administration;

(9) Ensuring all IT hardware procured is recorded in an official inventory tracking system (currently Sunflower) timely, accurately, and with supportable acquisition cost; and

(10) Ensuring all IT acquisitions include DHS and TSA Information Assurance (IA) requirements and Cyber Hygiene clause(s) where applicable.

G. The IT SSAC appointed by the CIO is responsible for:

(1) Supporting the CIO in implementing the requirements of FITARA, specifically, OMB M-15-14 Management and Oversight of Federal Information Technology, Attachment A, Common Baseline for IT Management and CIO Assignment Plan, Heading, Acquisition and Execution, Sub Heading, CIO Review and Approval of Acquisition, sections K1, and K2;

(2) Providing Senior-level technical review of every procurement, acquisition, solicitation, and agreement that contains an IT element for the appropriateness of the IT elements;

(3) Ensuring that appropriate ITAR Technical Evaluations are conducted for every phase of acquisition including Pre-Acquisition, Source Selection, and Pre-Award;

(4) Ensuring that the Technical Evaluation Team members have the appropriate level of subject matter expertise for the review under consideration;

(5) Providing oversight and direction to the Technical Evaluation Team for review; and

(6) Providing recommendations to the CIO prior to the CIO signature of all contract and agreement reviews.

H. The ITIRB is responsible for:

(1) Overseeing the management of the TSA IT portfolio, approving and prioritizing IT investments to best achieve TSA strategic goals and objectives, and leveraging opportunities for collaboration across TSA lines of business IT investments that support the TSA Mission and strategic objectives;

(2) Promoting the performance of key IT investments through visibility and proactive support by engaging specific expertise, leveraging efficiencies, and providing other value-added collaboration, insights, and resources;

(3) Improving effectiveness and reduce costs by leveraging agency-wide oversight, encouraging reuse of successful practices, and acting as an escalation point where appropriate; and

(4) Monitoring ongoing and proposed IT investments against their projected costs, schedule, and benefits, and directs programs to take corrective action to modify, or terminate programs, when necessary.

I. The EARC is responsible for:

(1) Ensuring all TSA investment and decision requests directly comply with TSA and DHS EA standards, mission, goals, and objectives;

(2) Ensuring the existence and practice of effective EA and standards, ITAR, CPIC, and SELC governance processes are in accordance with, and integral and aligned to the DHS architecture principles, the TSA EA and the DHS EA, and fully support the EA requirements of FITARA;

(3) Evaluating all TSA investment and decision request packages and making recommendations to the TSA ITIRB regarding the alignment of the investments with the TSA EA, consistent with criteria and thresholds identified by DHS; and

(4) Addressing DHS EA disposition and comments on request packages resulting from Department EA Review.

6. POLICY:

A. Documentation developed and maintained under the IT Governance framework shall be subject to all applicable TSA, DHS, and Federal policy for the identification and safeguarding of sensitive and classified information.

B. Disclosure of any documents under this directive outside of TSA by any party, regardless of the requestor, shall be fully coordinated with the TSA Office of Contracting and Procurement's (OCP), Civil Rights & Liberties, Ombudsman and Traveler Engagement (CRL/OTE), Chief Counsel (OCC), Finance and Administration (OFA), Office of Law Enforcement, Federal Air Marshal Service (OLE/FAMS) SSI Program, and OIT prior to responding to document data call requests.

C. All boards established or referenced in this directive shall be responsible for ensuring compliance with those actions stated herein.

D. The DR shall be based on a determination of mission need, completion of all required documentation, and will be subject to TSA ARB and/or TSA ITIRB review.

E. In order for the DR to be approved, all TSA programs and projects must adhere to the defined IT Governance processes and procedures.

F. The establishment of a centralized and consistent governance framework enables TSA investments to leverage new and existing capabilities, minimize costs, and meet OMB's funding requirements within an IT component. The IT Governance framework ensures TSA investments align IT strategic planning, EA, ITAR, CPIC, IT Portfolio Management, information assurance, IT Security, Privacy, DM, Systems Engineering, IT Operations, Risk Management, and Performance Management processes to directly support the delivery of TSA mission priorities.

G. The guidelines for adherence to the all processes stated herein (e.g., Acquisition Review, ITAR, CPIC, EA, SELC) must follow policies referenced in Section 3, Authorities.

7. PROCEDURES:

A. The procedures and required participants for the TSA EARC are identified in the TSA (EARC) Terms of Reference (TOR). Request reviews must follow the processes and procedures contained within this TOR.

B. The procedures and required participants for the TSA ITIRB are identified in the TSA (ITIRB) TOR. Request reviews must follow the processes and procedures contained within this TOR.

C. The procedures and required participants for the TSA IT SSAC are identified in the IT SSAC TOR. Request reviews must follow the processes and procedures contained within this TOR.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed ***April 3, 2017***

_____ _____

Russell Roberts
Assistant Administrator for Information
Technology/Chief Information Officer

Date

EFFECTIVE

_____

Date

Distribution: All TSA Employees and Contractors
Point-of-Contact: Office of Information Technology/Mission Support Division, 571-227-2019